Editorial Preface

Special Issue on Security and Privacy in Cloud Computing

Sang-Bing Tsai, Regional Green Economy Development Research Center, School of Business, Wuyi University, China & Research Center for Environment and Sustainable Development of the China Civil Aviation, China

This special issue of the Journal of Organizational and End User Computing (JOEUC) collects five articles. Dr. Marimuthu Karuppiah is affiliated with VIT University in India. Dr. Javier Medina Quero is affiliated with the University of Jaen in Spain. Dr. Xiong Li is affiliated with the Hunan University of Science and Technology in China. These guest editors provided support in the recruitment, consideration and publication of the following five titles.

The first article entitled "*A Novel Trust Model for Secure Group Communication in Distributed Computing"* presents an efficient TLADN (Trust Level Agreement for Distributed Network) trust evaluation method to detect the existence of malicious users in the distributed network and provided the trustworthiness among the users to perform dynamic secure group communication. Compared to existing schemes, the result shows three advantages of the proposed method which are higher trust accuracy and less storage space for maintaining the trust values and less communication complexity. In the future, a queuing model based on this trust model can be developed for better selection of secure optimal paths.

The second article entitled "Security-aware Autonomic Allocation of Cloud Resources: A Model, Research Trends and Future Directions" proposes a security-based resource allocation model for execution of cloud workloads called STARK in order to increase the security and reliability of cloud computing. The proposed STARK efficiently schedules the provisioned cloud resources for the execution of heterogenous cloud workloads and maintains the security of cloud services. Besides, the article also highlighted seven promising directions for future research in this field for hoping STARK model can be verified in real applications.

The third article entitled "An efficient Cloud Data Center allocation to the Source of requests" proposed an algorithm-modified Breadth First Search for efficiently allocating cloud data centers to source of requests by limiting the distance between them and keep the load of the cloud data center as balanced as possible. It is believed that compared with the existing modified Voronoi and K-Means approach, the proposed method has better performance in terms of in terms of average time taken, average cost and load distribution. Capacitated dominating sets with cloud data center allocation will further fine tune allocation problems by enabling load balancing of cloud data centers.

The fourth article entitled "A Risk Analysis Framework for Social Engineering Attack Based on User Profiling" contributes a risk analysis framework for social engineering attack based on user profiling for quantization calculation of social engineering attack vulnerability and risk. The modeling of user profile is based on extracting features related to social engineering attack. In this way, it is feasible to calculate the respectively vulnerability and risk of specific type of social engineering attack, the composite vulnerability and composite risk. Through examples and application analysis, the framework shows great extensions for the profiling features and defense factors can be extended to optimize the results or calculate unmentioned indicators.

The fifth article entitled "Android Botnets– A Proof-Of-Concept Using Hybrid Analysis Approach" proposes a hybrid analysis framework on the basis of two different steps which are code-based analysis and sandbox execution. In the first step, the authors analyzed and identified the existence of botnet phenomenon in Android-based mobile applications. Then, the authors highlighted all those permissions and API calls that can lead to a botnet activity and extracted them from a dataset comprising of ten applications to give the corresponding evaluation and conclusion. As the second step of the analysis task, the viability of the model was verified by sandbox testing and machine learning algorithms. In the future, some proactive mechanisms designed to defend botnets will be the focus of further research.

Sang-Bing Tsai
Editor-in-Chief
JOEUC